## III.   REMARKS

New claim 19 replaces original claim 1.  It positively recites "producing", which in turn includes "encrypting said first field by formatting", and it also recites specific details of the formatting.  Thus claim 19 includes all details and steps necessary or essential to the practice of the invention.  Further, claim 19 is supported by Figures 2 and 3, and paragraphs [0047] to [0090] of the description.  Also, "preferably" has been deleted wherever it occurs in the dependent claims, and new claims 20-23 recite the details formerly in the "preferably" clauses.

Thus all claims now satisfy 35 U.S.C. 112, first and second paragraphs.

Since claim 19 positively recites features and limitations of a method of producing an isolating identifier that is compatible with identifiers of a telephony network, it claims a method which produces a "useful, concrete and tangible result" (see MPEP 2106, IV, C, 2).  Thus it does not merely claim a data structure or only a mathematical operation.  Further, such a method is capable of causing functional change in a computer as explained in the description.  Hence there is no need to claim it as embodied in a computer-readable media.

Thus the claims are directed to statutory subject matter under 35 U.S.C. 101.

Regarding the specification, and, more particularly regarding the "NDS field" wording and the related telephony standard, please consider the following:
NDS: is a French usage of the Calling line Identification Presentation (CLIP) of the ISDN protocol (RNIS or Numeris for France), defined by the French Regulation authority ARCEP:  http://www.arcep.fr/fileadmin/reprise/dossiers/spectech/3-98_3-0.doc. (document in French).

However, the corresponding ETSI standards are ETSI ETS 300 356-3, 5 as provided hereafter.

ETSI ETS 300 356-3: 1995-02 DE/SPS-6001.08 Title: Integrated Services Digital Network (ISDN); Source: SPS 1 Signaling System No. 7; ISDN User Part (ISUP) version 2 for the International interface; 6 Pages Part 3: Calling Line Identification Presentation (CILP) supplementary service ETSI Price Code: A [ITU-T Recommendation Q.731, clause 3 (1993), modified].

ETSI ETS 300 356-4: 1995-02 DE/SPS-6001.09 Title: Integrated Services Digital Network (ISDN); Source: SPS 1 Signaling System No. 7; ISDN User Part (ISUP) version 2 for the International interface; 6 Pages Part 4: Calling Line Identification Restriction (CLIR) supplementary service ETSI Price Code: A [ITU-T Recommendation Q.731, clause 4 (1993), modified].

ETSI ETS 300 356-5: 1995-02 DE/SPS-6001.10 Title: Integrated Services Digital Network (ISDN); Source: SPS 1 Signaling System No. 7; ISDN User Part (ISUP) version 2 for the International interface; 6 Pages Part 5: Connected Line Identification Presentation (COLP) supplementary service ETSI Price Code: A [ITU-T Recommendation Q.731, clause 5 (1993), modified].

ETSI ETS 300 356-6: 1995-02 DE/SPS-6001.11 Title: Integrated Services Digital Network (ISDN); Source: SPS 1 Signaling System No. 7; ISDN User Part (ISUP) version 2 for the International interface; 5 Pages Part 6: Connected Line Identification Restriction (COLP) supplementary service ETSI Price Code: A [ITU-T Recommendation Q.731, clause 6 (1993), modified].

Thus it is submitted that the specification properly describes the invention in terms which are know in the art.

7

The claims are not unpatentable under 35 U.S.C. 103 over Asokan in view of what was obvious to a person of ordinary skill in the art.

The object of the claimed invention is a method for the <u>production of a multimedia isolating identifier by a service provider</u>. The field of the invention is that a user's access is that of the provider through a service provider. In particular, the field of the claimed invention is that of the gateways existing between telephone networks and Internet, voice or SMS networks, or other carriers for the transmission of multimedia or monomedia contents.

One of the main aims of the claimed invention is to **<u>preserve the user's privacy</u>**.

Another important aim of the claimed invention is <u>to preserve the customer database of the actors of a network, and to restrict activities of behavior analysis</u>.

Still another aim of the claimed invention is to contribute <u>to preserving the secrecy of mail or correspondence</u>.

Another aim of the claimed invention <u>is to enable an authorized legal entity to identify the civil status of a user</u>.

It is another aim of the claimed invention <u>is to enable the content provider to manage one or more contexts for users getting connected to said content provider</u>.

Also, it is another aim of the claimed invention <u>to remain compatible with the greatest number of networks</u>.

In the prior art, there are several means by which the content provider can identify a user who accesses one of his services. These means depend on the medium used by the user to access the service.

Mainly four modes of access can be distinguished, but the list is not exhaustive. A first mode of access is that of Internet-type access. The internet access mode can itself be divided into two sub-modes which may be called the connected mode and the unconnected mode. The connected Internet mode is a connection mode using an HTTP (Hyper Text Transfer Protocol) or WTP (Wireless Transfer Protocol) type of protocol. A server, for example, an HTTP server, is an apparatus communicating with a network, for example, the Internet, according to the HTTP protocol. Such a server hosts web (Internet) or WAP (Wireless Application Protocol) type networks. There is also an unconnected Internet access mode using an SMTP (Simple Mail Transfer Protocol) type protocol in which the connection actually consists of an exchange of mail-type electronic messages.

Another access mode is a mode of access by the operator. This mode itself is subdivided into two sub-modes. A first access sub-mode, which constitutes a third access mode, is then an access mode that may be called an unconnected mode. This mode uses an SMS (Short Message Service) or MMS (Multimedia Message Service) type protocol. A fourth access mode is a connected mode of access by operator also known as a voice mode in which the accessing user links up with a voice server.

All four access modes have a simple type of solution which consists in making an interface that proposes the keying in of an identifier and a password during a connection to a server. Inasmuch as the user linking up with the server of the content provider does so through a mobile telephone, the means made available to the user in order to key in his identifier (or login username) and password are limited by the user interface of the telephone. Either the identifier and the password are totally numerical, in which case they are difficult to memorize and easy to guess, or the identifier and the password are alphanumerical, in which case it is a tedious task to enter them with a keypad having only nine keys. Furthermore, this keying-in step is an additional step for

the user and, in most cases, discourages a mobile telephone user from linking up with a site that offers a connection interface of the type using an identifier and password.

Another approach, in the case of servers of the first type, consists in using a cookie. A cookie is a small file recorded in the user's machine. During a connection to a content provider, this content provider can access this cookie to identify the user. One problem with this approach lies in the fact that it is possible to steal a cookie by electronic or other means. The use of a cookie is therefore not compatible with high security requirements. Another problem then lies in the fact cookies have a relatively poor reputation. This incites the users to erase them. Furthermore, the user may configure the application, or navigator, that he uses to link up with the content provider, so that this application does not accept cookies. In this case, the user is unable to link up with the server of the content provider.

For the third and fourth access modes, the content provider usually has access to the telephone number of the person calling the server. The content provider is therefore capable of identifying the person through his telephone number. This is bound to raise a problem of protection of privacy. Indeed, it is quite legitimate for the user that he should wish not to be physically identified when he or she links up with the server of the content provider. Indeed, it should be possible to acquire an article anonymously. It is possible in this situation, to try and link up by masking one's number. However, in this case, it is impossible for the service to be invoiced and hence for the connection to be made effectively. At present, the only solution consists in not linking up with this content provider.

Furthermore, the prior art does not all resolve the problem of the format of the data. Indeed, the transmission characteristics are not the same from one network to another, and therefore from one protocol to another. These characteristics relate mainly to the encoding of the information transmitted (digital, alphanumerical and other information)

as well as the quantity of information that can be transmitted. Thus, an identifier that can be used on the Internet is not necessarily usable on a voice and/or SMS network.

In the specification, and in practice, getting connected to or accessing a content provider is equivalent to getting connected to a server of a content provider.

The claimed invention resolves these problems by enabling the production of an identifier that the user presents to the content provider, whatever the type of network. This identifier enables no one, other than the entity having produced this identifier, to identify the civil status of the user. (This is the actual meaning of the wording "isolating"). Such an identifier makes it possible to protect the user's privacy and enables the user to be properly identified through a request produced by the authority seeking to identify the user and comprising the identifier as well as the date on which this identifier is produced.

An identifier according to the claimed invention comprises at least one first user identifier field. Other fields may ensure the variability of the identifier, and/or the qualification of the identifier. This variability is ensured either by a random variable, or by a stated desire of the user. The qualification of the identifier consists of information used to give interpretation clues relating to the nature of the identifier. Such clues are, for example, the operator that has produced the identifier, the lifetime of the identifier, etc. The first field is encrypted so that this first field is accessible to no one. Only the service provider, namely the entity producing the isolating identifier, is capable of inverting the encryption and therefore of physically identifying to the user.

All the fields of the identifier according to the claimed invention, including the encrypted fields, are in a format compatible with the most constraint-bound of the networks in which the identifier has to be conveyed. In practice, this condition pertains to the telephony network and its constraints for defining an identifier. The telephony network indeed imposes a maximum length and a digital encoding for the identifier.

11

The claimed invention so relates to a <u>producing an isolating identifier</u>. An identifier is so created by assembling fields having the claimed specific properties. These properties are given by the construction of said identifier.

New claim 19 recites the properties given to the created identifier by the claimed method. As the identifier is a complex entity, i.e., an entity comprising several properties, all these properties are given in a unique step, which is the step 303 or 304 in the specification. This step is, in fact in the specification, a sub-step of a larger method to identify a user on a network. But as a step it is, of course, also a method and this method comprises in precisely creating (computing) the isolating identifier of a multimedia user.

The aims of the claimed invention are therefore truly, fully and efficiently achieved by the claimed method producing a first isolating identifier of a multimedia user that is compatible with identifiers of a telephony network, said identifier having at least one first user identifier field, said producing including encrypting said first field by formatting the first isolating identifier in the following format:

-the first identifier comprises N identifier digits for designating the user,

-the first identifier comprises at least one nature digit for defining the nature of the first identifier, and

-the first identifier comprises M variability digits,

wherein:

-the M variability digits depends on the nature digit,

-the first identifier has a maximum size of 15 digits, one digit being a computer representation for representing/encoding a decimal or hexadecimal digit and comprising 4 bits, and

-the first identifier comprises at least one producer digit for designating the producer of the identifier.

In this way, this claimed invention successfully solves all the problems relating to security, confidence of users and ergonomics consideration.

Contrary to what the claimed invention teaches, i.e., "how to efficiently and easily preserve the user's privacy" and this being the main purpose of the claimed invention, the unique purpose of Asokan is to propose a method for a mobile phone to acquire an IP network address in a communications network according to Ipv4 or Ipv6.

According to Asokan, an IP static or dynamic IP address is provided, but this one is fully known and this is exactly what the claimed invention wishes to avoid. The claimed invention enables efficiently hiding the user's identity, said identity being replaced by the isolating identifier. This prevents a third party, except the provider and only the provider of this identifier, that is to say the access provider, from knowing the true identity of the user.

As a good example, the following excerpt from the specification at page 17 will allow to better understand the nature, purpose and advantages of the claimed invention.

"[0084] One advantage of the invention and of the isolation context identifiers defined by it is that one user can have a different context identifier for each content provider. It is thus impossible for a content provider to collate his databases of other content providers so as to obtain more knowledge about the private lives of users identified by the identifier. It is also impossible to raid a database, or infringe the secrecy of communications. Thus, maximum protection is obtained for the user's privacy.

[0085] The legal requirements are also met since, starting from an identifier and only for the operator who has produced this identifier, it is possible to trace an operation back to the physical user."

Asokan teaches exactly the contrary. The present description at page 7, paragraph [0042], will help to better measure the huge differences between both disclosures. Within this paragraph it is clearly said: "One role of the gateway 112 is to set up the link between the identifier 117 and the isolating identifier 118". Also: "Such an identifier 117 is a public identifier that enables everybody to associate a physical person with it". As a matter of fact, the identifier in Asokan fully corresponds to the identifier 117 and never to the presently claimed isolating identifier 118. Nowhere in Asokan is the claimed isolating identifier disclosed, Asokan disclosing exactly the contrary. Thus it is respectfully submitted that Asokan and the claimed invention are not directed to the same issues.

It is noted that Official Notice of what is obvious to one of ordinary skill in the art can only be taken of facts that are capable of "instant and unquestionable demonstration: (MPEP 2144.03 (A)), which is not the present case due to the highly complex technology involved herein. Thus the Examiner is asked to provide a reference for these asserted facts (MPEP 2144.03(c)). Since the above discussed claim limitations are disclosed in neither Asokan nor what is obvious to a person of ordinary skill in the art, combining them does not result in the claimed invention. Thus the above rejection should be withdrawn.

Claims 15-16 are not unpatentable under 35 U.S.C. 103(a) over Asokan in view of what was obvious to a person of ordinary skill in the art further in view of Ginzboorg.

Since Ginzboorg does not disclose the above-discussed features, combining it with the first two references does not result in the claimed invention. Thus this rejection should be withdrawn.
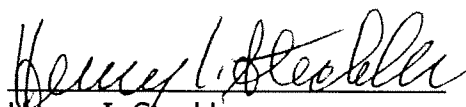
Claims 11-14, 17-18 are not unpatentable under 35 U.S.C. 103(a) over Asokan in view of what was obvious to a person of ordinary skill in the art further in view of Brainard.
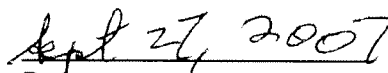
Similarly, Brainard fails to disclose the above-discussed features. Thus this rejection should be withdrawn.

For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record, and are in proper form for allowance. Accordingly, favorable reconsideration and allowance is respectfully requested. Should any unresolved issues remain, the Examiner is invited to call Applicants' attorney at the telephone number indicated below.

The Commissioner is hereby authorized to charge payment for any fees associated with this communication or credit any over payment to Deposit Account No. 16-1350.

Respectfully submitted,

_Henry I. Steckler_

Henry I. Steckler
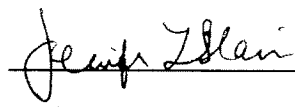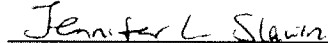Reg. No. 24,139

_Sept 27, 2007_
Date

Perman & Green, LLP
425 Post Road
Fairfield, CT  06824
(203) 259-1800
Customer No.: 2512

## CERTIFICATE OF ELECTRONIC FILING

I hereby certify that this correspondence is being transmitted electronically, on the date indicated below, addressed to the Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA  22313-1450.

Date: 3-October-2007          Signature: _Jennifer Slavin_

_Jennifer L Slavin_
Person Making Deposit